

- [54] **DESCRAMBLER SUBSCRIBER KEY  
PRODUCTION SYSTEM UTILIZING KEY  
SEEDS STORED IN DESCRAMBLER**
- [75] **Inventor:** **Karl E. Moerder, Poway, Calif.**
- [73] **Assignee:** **M/A-COM Government Systems,  
Inc., San Diego, Calif.**
- [\*] **Notice:** **The portion of the term of this patent  
subsequent to Sep. 23, 2003 has been  
disclaimed.**
- [21] **Appl. No.:** **589,741**
- [22] **Filed:** **Mar. 15, 1984**
- [51] **Int. CL<sup>4</sup> .....** **H04L 9/00**
- [52] **U.S. CL. ....** **178/22.14; 178/22.17;  
178/22.15; 178/22.09; 358/122**
- [58] **Field of Search .....** **178/22.09, 22.13, 22.15,  
178/22.11, 22.16, 22.14; 358/114, 122, 124**

[56] **References Cited**

## U.S. PATENT DOCUMENTS

3,659,046	4/1972	Angeleri et al. ....	178/22.13
3,911,216	10/1975	Bartek et al. ....	178/22.15
3,914,534	10/1975	Forbes .....	358/122
4,058,830	11/1977	Guinet et al. ....	358/114
4,168,396	9/1979	Best .....	178/22
4,200,770	4/1980	Hellman et al. ....	178/22.11
4,292,650	9/1981	Hendrickson .....	358/122
4,323,921	4/1982	Guillou .....	358/114
4,337,483	6/1982	Guillou .....	358/114
4,354,201	10/1982	Sechet et al. ....	358/122
4,365,110	12/1982	Lee et al. ....	78/22.09
4,388,643	6/1983	Aminetzah .....	358/123
4,461,032	7/1984	Skerlos .....	455/4
4,467,139	8/1984	Mollier .....	178/22.08
4,471,164	9/1984	Henry .....	178/22.11
4,484,027	11/1984	Lee et al. ....	178/22.13
4,531,020	7/1985	Wechselberger et al. ....	358/122

4,531,021 7/1985 Bluestein et al. .... 358/122

**Primary Examiner—Salvatore Cangialosi**

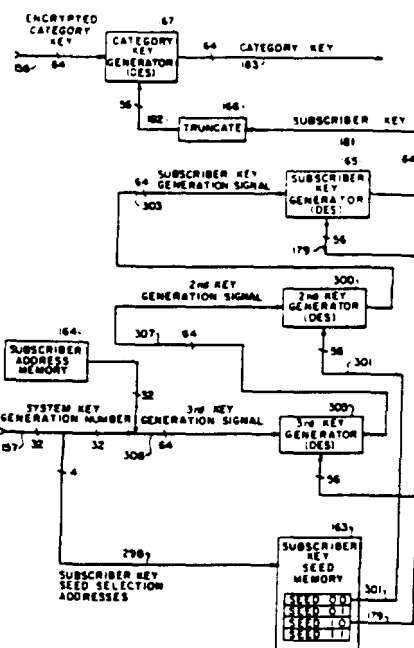
Assistant Examiner—Aaron J. Lewis

Attorney, Agent, or Firm—Edward W. Callan

## [57] ABSTRACT

A system for reproducing in a descrambler of a subscriber communication network a subscriber key signal that is unique to the descrambler and was used in encrypting a key signal that must be decrypted for use in descrambling a signal received by the descrambler. The scrambled signal is received by the descrambler together with the encrypted key signal and a key generation number containing an address for accessing a predetermined area in a memory contained in the descrambler. The system includes a circuit for providing a subscriber key generation signal that is unique to the descrambler; a subscriber key generator for reproducing the unique subscriber key signal by processing the subscriber key generation signal in accordance with a predetermined encryption algorithm upon the algorithm being keyed by a prescribed subscriber key seed signal that is unique to the descrambler; a secure memory storing a plurality of different subscriber key seed signals, and for providing the prescribed seed signal to key the algorithm when the area of the memory containing the prescribed seed signal is accessed by the address contained in the received key generation number; and a circuit for accessing the first memory with the address contained in the received key generation number. The subscriber key generation signal is formed by combining the received key generation number with a unique subscriber address signal that is stored in a second memory of the descrambler.

**24 Claims, 4 Drawing Figures**



- [54] SELECTIVE-SUBSCRIPTION  
DESCRAMBLING
- [75] Inventors: Kleia S. Gilhousen; Jerrold A. Heller;  
Michael Van Harding, all of San  
Diego; Robert D. Blakeney, II, Del  
Mar, all of Calif.
- [73] Assignees: M/A-COM Government Systems,  
Inc.; Cable/Home Communication  
Corp., both of San Diego, Calif.
- [21] Appl. No.: 618,917
- [22] Filed: Jan. 8, 1984
- [51] Int. Cl.<sup>4</sup> ..... H04N 7/167; H04N 7/00;  
H04L 9/00
- [52] U.S. Cl. .... 380/20; 340/825.33;  
340/825.34; 358/84; 380/23; 380/29; 380/44;  
380/45
- [58] Field of Search ..... 358/122, 115, 84;  
455/2; 340/825.33, 825.34; 178/22.13; 380/20,  
23, 29, 44, 45

[56] References Cited

U.S. PATENT DOCUMENTS

2,573,349	10/1951	Miller et al.	177/353
2,788,387	4/1957	Druz	178/5.1
2,864,885	12/1958	Morris	178/5.1
2,866,962	12/1958	Ellett	340/147
3,016,091	9/1962	Kirk, Jr. et al.	178/5.1
3,331,586	9/1970	Bass et al.	178/6
3,736,369	5/1973	Vogelman et al.	178/5.1
3,882,392	5/1975	Harney	325/33
3,886,302	5/1975	Kosco	178/5.1
3,890,461	6/1975	Vogelman et al.	178/5.1
3,934,079	1/1976	Barnhart	455/2
3,956,615	5/1976	Anderson et al.	235/61.7
3,997,718	12/1976	Ricketts et al.	178/6.8
4,068,264	1/1978	Pires	358/122
4,115,807	9/1978	Pires	358/122
4,130,833	12/1978	Chomet	358/122
4,163,254	7/1979	Block et al.	358/122
4,163,255	7/1979	Pires	358/122
4,225,884	9/1980	Block	358/122
4,245,245	1/1981	Matsumoto et al.	358/122
4,323,922	4/1982	den Toonder et al.	358/117
4,388,643	6/1983	Aminetzah	358/122
4,434,436	2/1984	Kleykamp et al.	358/118
4,475,123	10/1984	Dumbauld et al.	358/114

4,484,027	11/1984	Lee et al.	358/122
4,484,217	11/1984	Block et al.	358/84
4,486,773	12/1984	Okubo	358/84
4,528,589	7/1985	Block et al.	358/122
4,531,021	7/1985	Blucstein et al.	358/122
4,535,355	8/1985	Arn et al.	358/123
4,536,791	8/1985	Campbell et al.	358/122

OTHER PUBLICATIONS

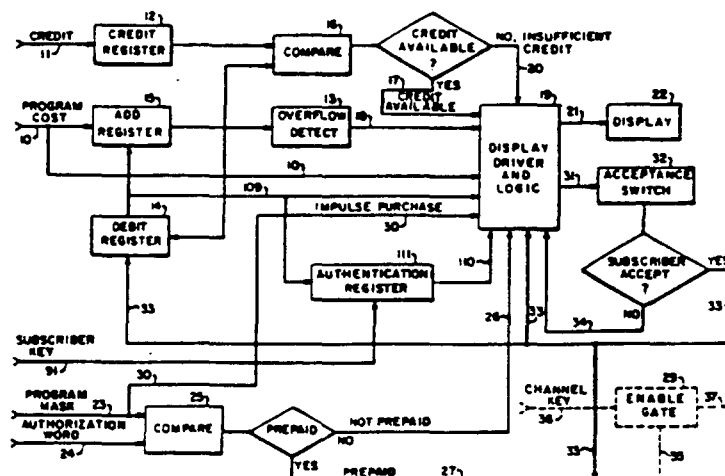
PCT Patent Application WO83/04154; Block, Robert S. and Lull, John M. 05/11/82; "Method and System for Remote Reporting, Particularly for Pay Television Billing".

Primary Examiner—Stephen C. Buczniski  
Attorney, Agent, or Firm—Edward W. Callan

[57] ABSTRACT

A system in a subscriber television network for enabling descrambling of a received scrambled signal on a prepaid basis and/or an impulse-purchase basis. A received mask signal uniquely related to the scrambled signal is compared with a received authorization signal indicating whether the subscriber is authorized to receive the scrambled signal on a prepaid basis and a prepaid signal for enabling descrambling is provided when the compared signals match. A not-prepaid signal is provided when they do not match. A received cost signal indicating the charge for descrambling the scrambled signal and a received credit signal indicating only the subscriber's accumulated credit are processed with reference to a stored record of the subscriber's prior accumulated charges to determine whether the subscriber has sufficient available credit to pay for descrambling of the scrambled signal. If a program is not prepaid and if sufficient credit is available, the subscriber is given the option of causing the signal to be descrambled on an impulse-purchase basis. To prevent a subscriber from obtaining descrambling through such deceit as changing the mask, authorization, cost and/or credit signals, these signals are processed with key signals which are used in scrambling and descrambling the television signal such that descrambling is prevented if any of the mask authorization, cost and/or credit signals is changed.

6 Claims, 4 Drawing Figures



- [54] **SELECTIVE ENABLEMENT OF  
DESCRAMBLERS**
- [75] Inventors: Klein S. Gilhousen; Jerrold A. Heller;  
Michael V. Harding, all of San  
Diego; Robert D. Blakeney, II, Del  
Mar, all of Calif.
- [73] Assignees: M/A-COM Government Systems  
Inc.; Cable/Home Communication  
Corporation, both of San Diego,  
Calif.
- [\*] Notice: The portion of the term of this patent  
subsequent to Dec. 8, 2004 has been  
disclaimed.
- [21] Appl. No.: 128,889
- [22] Filed: Dec. 4, 1987

**Related U.S. Application Data**

- [62] Division of Ser. No. 618,917, Jun. 8, 1984, Pat. No.  
4,712,238.
- [51] Int. CL<sup>4</sup> ..... H04N 7/167; H04N 7/00;  
H04L 9/00
- [52] U.S. CL ..... 380/24; 340/825.33;  
340/825.34; 358/84; 380/20; 380/23; 380/29;  
380/45; 455/2
- [58] Field of Search ..... 358/84; 455/2;  
340/825.33, 825.34; 380/20, 23, 29, 44, 45, 24
- [56] **References Cited**

**U.S. PATENT DOCUMENTS**

- 2,573,349 10/1951 Miller et al. .  
2,788,387 4/1957 Druz .  
2,864,885 12/1958 Morris .  
2,866,962 12/1958 Ellett .  
3,016,091 9/1962 Kirk, Jr. et al. .  
3,531,586 9/1970 Bass et al. .  
3,736,369 5/1973 Vogeliman et al. .  
3,882,392 5/1975 Harney .  
3,886,302 5/1975 Kosco .  
3,890,461 6/1975 Vogeliman et al. .  
3,934,079 1/1976 Barnhart .  
3,956,615 5/1976 Anderson et al. .  
3,997,718 12/1976 Ricketts et al. .  
4,068,264 1/1978 Pires .  
4,115,807 9/1978 Pires .  
4,130,833 12/1978 Chomet .  
4,163,254 7/1979 Block et al. .  
4,163,255 7/1979 Pires .

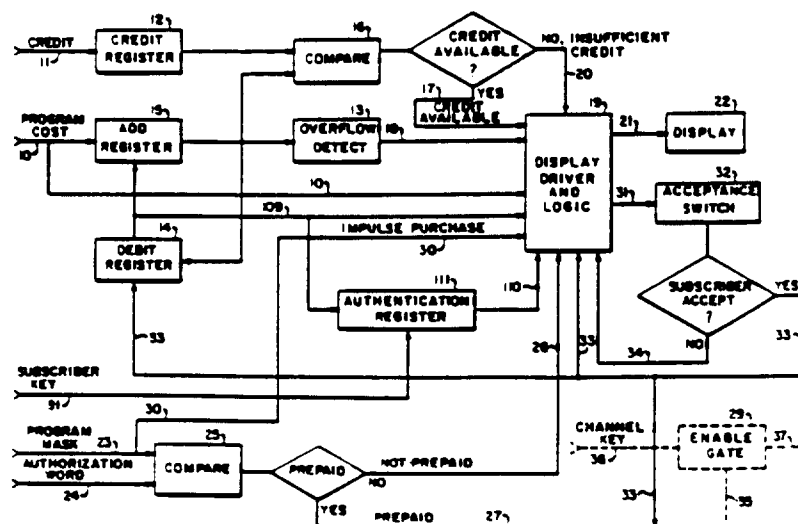
- 4,225,884 9/1980 Block .  
4,245,245 1/1981 Matsumoto et al. .  
4,323,922 4/1982 Den Toonder et al. .  
4,388,643 6/1983 Aminetzah .  
4,434,436 2/1984 Kleykamp et al. .  
4,475,123 10/1984 Dumbauld et al. .  
4,484,027 11/1984 Lee et al. .  
4,484,217 11/1984 Block et al. .... 358/84  
4,486,773 12/1984 Okubo ..... 358/84  
4,528,589 7/1985 Block et al. .  
4,531,020 7/1985 Wechseiberger et al. .... 380/20  
4,531,021 7/1985 Bluestein et al. .  
4,535,355 8/1985 Arn et al. .  
4,536,791 8/1985 Campbell et al. .

**FOREIGN PATENT DOCUMENTS**

- 8304154 5/1982 World Int. Prop. O. .  
*Primary Examiner*—Stephen C. Buczinski  
*Attorney, Agent, or Firm*—Edward W. Callan  
[57] **ABSTRACT**

A system in a subscriber television network for enabling descrambling of a received scrambled signal on a pre-paid basis and/or an impulse-purchase basis. A received mask signal uniquely related to the scrambled signal is compared with a received authorization signal indicating whether the subscriber is authorized to receive the scrambled signal on a prepaid basis and a prepaid signal for enabling descrambling is provided when the compared signals match. A not-prepaid signal is provided when they do not match. A received cost signal indicating the charge for descrambling the scrambled signal and a received credit signal indicating the subscriber's endlessly accumulated credit are processed with reference to a stored record of the subscriber's prior accumulated charges to determine whether the subscriber has sufficient available credit to pay for descrambling of the scrambled signal. If a program is not prepaid and if sufficient credit is available, the subscriber is given the option of causing the signal to be descrambled on an impulse-purchase basis. To prevent a subscriber from obtaining descrambling through such deceit as changing the mask, authorization, cost and/or credit signals, these signals are processed with key signals which are used in scrambling and descrambling the television signal such that descrambling is prevented if any of the mask et al authorization, cost and/or credit signals is changed.

21 Claims, 4 Drawing Sheets



## [54] REPRODUCTION OF SECURE KEYS BY USING DISTRIBUTED KEY GENERATION DATA

[75] Inventors: Christopher J. Bennett; Michael V. Harding, both of San Diego; Paul Moroney, Cardiff-by-the-Sea, all of Calif.

[73] Assignee: General Instrument Corporation, New York, N.Y.

[21] Appl. No.: 200,111

[22] Filed: May 27, 1988

[51] Int. Cl.<sup>4</sup> ..... H04L 9/02

[52] U.S. Cl. .... 380/21; 380/20;

380/47

[58] Field of Search ..... 380/20, 21, 45, 47

## [56] References Cited

## U.S. PATENT DOCUMENTS

4,613,901	9/1986	Gilhausen et al.	380/20
4,634,808	1/1987	Moerder	380/20
4,694,491	9/1987	Horne et al.	380/20
4,712,238	12/1987	Gilhausen et al.	380/20
4,736,422	4/1988	Mason	380/20
4,792,973	12/1988	Gilhausen et al.	380/20

## OTHER PUBLICATIONS

Denning, "Cryptography and Data Security" Addison Wesley, 1982, pp. 14-16, 161-164, 169-171.

"Specification for Conditional Access Receivers", Draft NR-MSK Specification Vedlegg 4, Oct. 1987, pp. 40-44.

Primary Examiner—Salvatore Cangialosi

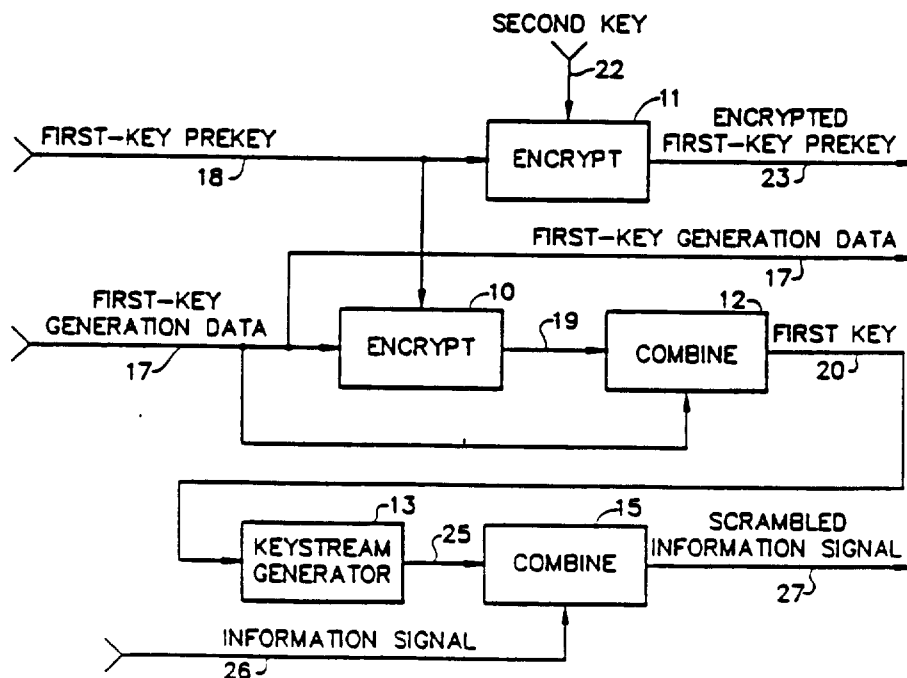
Attorney, Agent, or Firm—Edward W. Callan

## [57] ABSTRACT

A key security system provides for the reproduction of secure keys by using distributed key generation data and a distributed encrypted prekey. The system en-

crypts program key generation data with a program key prekey in accordance with a first encryption algorithm to produce the program key; processes the program key to produce a keystream; and processes an information signal with the keystream to produce a scrambled information signal. The program key prekey is encrypted with a category key in accordance with a second encryption algorithm to produce an encrypted program key prekey. The scrambled information signal, the program key generation data and the encrypted program key prekey are distributed to descramblers. The descrambler within the key security system decrypts the distributed encrypted program key prekey with the category key in accordance with the second encryption algorithm to reproduce the program key prekey; encrypts the distributed program key generation data with the reproduced program key prekey in accordance with the first encryption algorithm to produce the program key; processes the reproduced program key to reproduce the keystream; and processes the distributed scrambled information signal with the reproduced keystream to descramble the distributed scrambled information signal. The key generation data includes authorization data that must be processed by the authorization processor in the descrambler in order to enable the descrambler. The use of authorization data as key generation data protects the authorization data from spoofing attacks. When more data must be protected than a single operation of the encryption algorithm can support, then additional data blocks are protected by chaining the system, wherein the output from one stage forms part of the input to the next. The key generation data for the program key includes a sequence number securely associated with the category key to thereby "timelock" program key reproduction to the use of a current category key and thus prevent an attack based upon the use of an obsolete category key.

24 Claims, 9 Drawing Sheets



[54] **SECURE INTEGRATED CIRCUIT CHIP WITH CONDUCTIVE SHIELD**

[75] Inventors: Robert C. Gilberg; Richard M. Knowles, both of San Diego; Paul Moroney, Cardiff-by-the-Sea; William A. Shumate, San Diego, all of Calif.

[73] Assignee: General Instrument Corporation, New York, N.Y.

[21] Appl. No.: 297,472

[22] Filed: Jan. 12, 1989

[51] Int. Cl.<sup>3</sup> ..... G11C 7/00; G06F 13/00

[52] U.S. Cl. .... 365/53; 365/63; 365/226; 365/225.7; 307/202.1; 380/3; 357/85

[58] Field of Search ..... 365/52, 53, 63, 218, 365/228, 225.7, 226; 307/202.1; 357/85; 340/652; 380/3, 4

[56] **References Cited**

**U.S. PATENT DOCUMENTS**

3,882,323	5/1975	Smolker	307/202.1
4,593,384	6/1986	Kleijne	365/228
4,811,288	3/1989	Kleijne et al.	365/52

**FOREIGN PATENT DOCUMENTS**

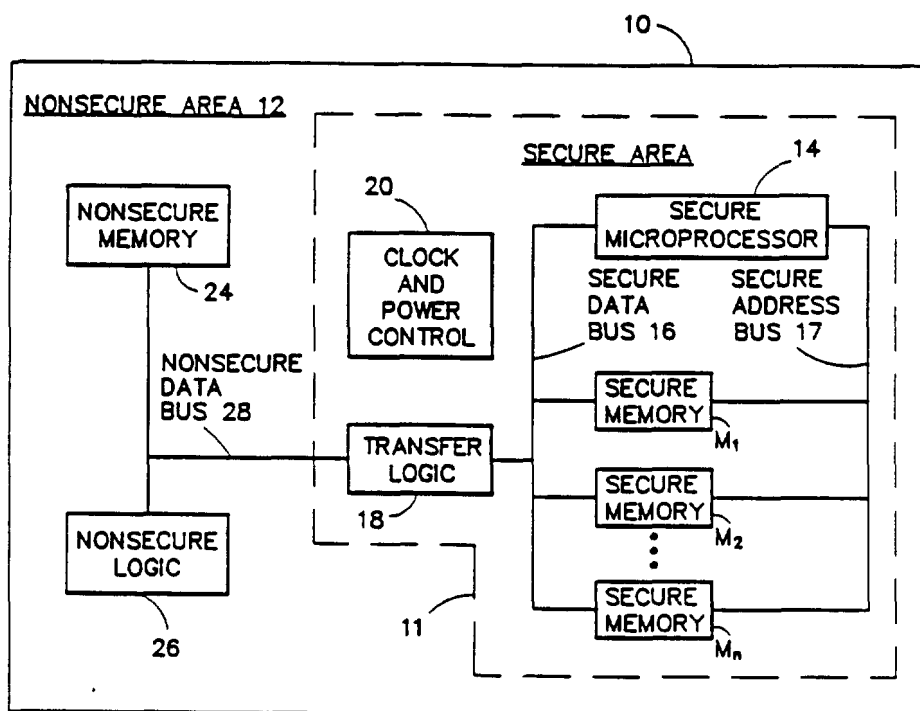
WO84/04614 11/1984 PCT Int'l Appl. .

Primary Examiner—Joseph A. Popek  
Attorney, Agent, or Firm—Edward W. Callan

[57] **ABSTRACT**

An integrated circuit chip containing a secure area in which secure data is processed and/or stored, includes a semiconductive layer containing diffusions defining circuit element components; a first conductive layer coupled to the semiconductive layer to interconnect the components to thereby define circuit elements for distributing, storing processing and/or affecting the processing of secure data; and a second conductive layer overlying the circuit elements to thereby define a secure area in which the circuit elements are shielded from inspection, and coupled to the circuit elements for conducting to the circuit elements a predetermined signal that is essential to an intended function of the shielded circuit elements, whereby removal of the second conductive layer will prevent the predetermined essential signal from being provided to the circuit elements and thereby prevent the intended function.

25 Claims, 5 Drawing Sheets



## **APPENDIX 2**

### **LETTER FROM RSA LABORATORIES**

30 MARINE PARKWAY  
HOLLYWOOD CITY,  
CA 91605

January 13, 1993

MR. CHUCK NEWBY  
Project Engineer  
Titan Satellite Systems Corporation  
3033 Science Park Road  
San Diego, CA 92121

Dear Chuck:

You asked me for an opinion on whether HBI transmission of the Linkabit Smart Card System's<sup>1</sup> control channel is more or less secure than VBI transmission, and whether the coexistence of the Linkabit Smart Card System and General Instrument's VideoCipher II Plus<sup>2</sup> system weakens security.

#### HBI vs. VBI

HBI transmission of a digital control channel is intrinsically no more or less secure than VBI transmission. Cryptographic security depends on how the bits are protected, not on special analog characteristics of the interval. Whether the control channel is in the HBI or VBI has no impact on the difficulty of obtaining keys.

---

<sup>1</sup>Linkabit Smart Card System is a trademark of Titan Satellite Systems Corporation.

<sup>2</sup>VideoCipher II and VideoCipher II Plus are registered trademarks of General Instrument Corporation.

The fact that the VideoCipher II control channel is in the HBI and VideoCipher II descramblers are easily "pirated" may suggest to some that the HBI is easily pirated. But VideoCipher II piracy has nothing to do with HBI or VBI transmission. It has everything to do with weaknesses in the descrambler's physical security.

VideoCipher II descrambler hardware, which reads the HBI, is easily adapted to read TSSC's control channel, which is in the HBI. But the descrambler hardware is also easily modified to read the VideoCipher II Plus control channel, which is in the VBI. The only difference between HBI and VBI is the location of samples within a video frame. Once existing descrambler hardware achieves "frame sync," it seems reasonable that inexpensive new hardware with built-in timers can find and sample the VBI. A descrambler is therefore "raw material" for either Linkabit piracy or VideoCipher II Plus piracy—if the pirate breaks one or the other system.

HBI transmission of the Linkabit Smart Card System's control channel is therefore no more or less secure than VBI transmission. VideoCipher II Plus and the Linkabit Smart Card System are on equal ground. The security of both systems depends on cryptographic protocols and physical implementation, not on HBI or VBI.

#### Multiple security systems

The coexistence of multiple security systems with common cryptographic keys raises important concerns. The security of any system, it is often said, is only as high as the lowest fence. A pirate will attack whichever system is weakest.

Two provisions are essential. Fence "height" must be measurable, to some degree; a security provider with a low fence should not be permitted to interoperate. And fence "crossings" must be detectable. If a pirate does attack a system, it should be possible to determine which system the pirate attacked.

Titan Satellite has retained RSA Laboratories and XTBC to review the security of the Linkabit Smart Card System, covering both cryptographic protocols and physical implementation. While no one can guarantee a system's security, the results of the review should provide a good

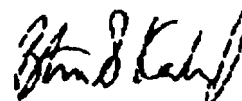


measuring sticks. As Titan discloses details of the system to other reviewers, the measurement will become more accurate.

The Linkabit Smart Card System and VideoCipher II (and II Plus) interoperate only at the channel encryption level, not at the conditional access/key management levels. It is generally not practical to attack a system at the channel encryption level because the channel encryption key changes so frequently. An attack on either system will therefore, most likely, involve not the interoperable parts, but the different parts. Pirated descramblers will contain software and keys implementing one system or the other. It follows that fence crossings can be detected.

Coexistence of the Linkabit Smart Card System and General Instrument's VideoCipher II Plus system therefore does not necessarily weaken security. Indeed, it is possible that the introduction of new systems, properly reviewed, will strengthen security overall.

Sincerely,



Burton S. Kaliski Jr., Ph.D.  
Chief Scientist